

REMARKS


Prior to examination of the above-referenced application, entry of the above amendments and new claims is respectfully requested to round out the scope of protection to which applicants are entitled. No new matter is added.

Early examination on the merits are respectfully requested.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By:


Gordon Kessler
Registration No. 38,511
Tel. (212) 588-0800

09872509-060101
T0T030" 60527860

APPENDIX

MARKED-UP CLAIMS

1. (Amended) An enciphering apparatus for enciphering data using a cryptographic key, comprising:

[enciphering means for enciphering data using a cryptographic key;]

first [generating] providing means for [generating] providing a first [key] information which is changed during a predetermined session;

second providing [generating] means for providing [generating] a second [key] information which is changed [at a] during the predetermined session [timing while the data is enciphered]; [and]

producing means for producing a [the] cryptographic key [using] based on the first [key] information which is changed during the predetermined session and the second [key] information which is changed during the predetermined session; and

enciphering means or enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

3. (Amended) An enciphering apparatus according to claim 1, wherein said producing means produces [a] said cryptographic key with which a correct decipherment result is obtained even if the first [cryptographic key] information and the second

[cryptographic key] information which [compose the] are used to generate said cryptographic key are used individually to successively decipher the enciphered data.

4. (Amended) An enciphering apparatus according to claim 1, wherein said producing means adds the second [key] information to a value whose initial value is the first [key] information to produce the cryptographic key.

5. (Amended) An enciphering apparatus according to claim 4, wherein the first [key] information has a number of bits larger than that of the second [key] information, and said producing means adds the second [key] information to bits at predetermined positions of the first [key] information, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

9. (Amended) An enciphering method for enciphering data using a cryptographic key, comprising the steps of:

[enciphering data using a cryptographic key;]

[generating] providing a first [key] information which is changed during a predetermined session;

[generating] providing a second [key] information which is changed [at a] during the predetermined session; [timing while the data are enciphered; and]

producing [the] a cryptographic key [using] based upon the first [key] information which is changed during said

predetermined session and the second [key] information which is changed during the predetermined session; and

enciphering data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

10. (Amended) A deciphering apparatus for deciphering data using a cryptographic key, comprising:

receiving means for receiving enciphered data;

[deciphering means for deciphering the received data using a cryptographic key;]

first [generating] providing means for [generating] providing a first [key] information which is changed during a predetermined session;

second [generating] providing means for [generating] providing a second [key] information which is changed [at a during the predetermined session; [timing while the data is deciphered; and]

producing means for producing [the] a cryptographic key [using] based upon the first [key] information which is changed during the predetermined session and the second [key] information which is changed during the predetermined session; and

deciphering means for deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key

is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

11. (Amended) A deciphering apparatus according to claim 10, wherein said producing means includes first producing means for producing a first cryptographic key [using] based upon one of the first [key] information and the second [key] information, and second producing means for producing a second cryptographic key [using] based upon the other of the first [key] information and the second [key] information, and said deciphering means includes first deciphering means for deciphering the enciphered data [using] based upon the first cryptographic key, and second deciphering means for deciphering the data deciphered by said first deciphering means further [using] based upon the second cryptographic key.

13. (Amended) A deciphering method for deciphering data using a cryptographic key, comprising the steps of:

receiving enciphered data;

[deciphering the received data using a cryptographic key;]

[generating] providing a first [key] information which is changed during a predetermined session;

[generating] providing a second [key] information which is changed [at a] during the predetermined session; [timing while the data is deciphered; and]

producing [the] a cryptographic key [using] based upon the first [key] information which is changed during the predetermined

session and the second [key] information which is changed during the predetermined session; and

deciphering said received enciphered data using said cryptographic key, wherein said cryptographic key is changed at a predetermined timing during the predetermined session in accordance with a change in said second information.

16. (Amended) An information processing apparatus, comprising:

receiving means for receiving enciphered data transmitted thereto through a bus;

producing means composed of a software program for producing a first cryptographic key and a second cryptographic key [which is changed at a predetermined timing while the data is deciphered from the data received by said receiving means] based upon a first information which is changed during a predetermined session and a second information which is changed during the predetermined session;

first deciphering means for deciphering the enciphered data received by said receiving means using one of the first cryptographic key and the second cryptographic key produced by said producing means; and

second deciphering means for deciphering and processing the data deciphered by said first deciphering means further using the other of the first cryptographic key and the second cryptographic

key produced by said producing means, wherein said second cryptographic key is changed while said data is being deciphered.

17. (Amended) An information processing method, comprising the steps of:

receiving enciphered data transmitted thereto through a bus;
producing, from the received data, a first cryptographic key, and a second cryptographic key based upon a first information which is changed during a predetermined session and a second information which is changed during the predetermined session [which is changed at a predetermined timing while the data is deciphered];

deciphering the received enciphered data using one of the first cryptographic key and the second cryptographic key; and

deciphering the deciphered data further using the other of the first cryptographic key and the second cryptographic key, wherein said second cryptographic key is changed while said data is being deciphered.

FOF030"60524860

"Express Mail" mailing label number EL 742697388 US

Date of Deposit June 1, 2001

I hereby certify that this paper or fee, and a patent application and accompanying papers, are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and are addressed to the Assistant Commissioner for Patents, Washington, DC 20231.

Charles Jackson

(Typed or printed name of person mailing paper or fee)

Charles Jackson

(Signature of person mailing paper or fee)

FORM 6052-860